Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Note

Security in Android smartphone, Confidentiality in IoT-enabled Smart Grids, and Fault-tolerant privacy-preserving in AMS

Deliverable D0.9

Note no. DART/07/20

Authors Habtamu Abie, Svetlana Boudko, Sigurd Eskeland

Date 3. des. 2020

Authors

Habtamu Abie, PhD, is currently a Chief Research Scientist at NR. He received his B.Sc., M.Sc. and Ph.D. from the University of Oslo, and has many years of experience in computing, both as practitioner and researcher. He has a solid and extensive background in the design and development of real-time systems, and the design, modelling and development of security for distributed computing systems. He is NR's principal investigator of the IoTSec project and WP leader.

Svetlana Boudko, PhD, is currently a Senior Research Scientist at NR. She received her M.Sc. from Moscow Aviation Institute and Ph.D. from the University of Oslo and has been engaged in various research and development projects. Her interests include modelling and analysis, distributed systems, game theory, multi-agent systems, and machine learning. In the IoTSec project, she modelled and analysed security attacks and defences in advanced metering infrastructures and developed adaptive data collection for real-time security analytics.

Sigurd Eskeland has more than 20 years of experience in information security with special interests in public key cryptography and cryptographic protocols. He is currently a researcher at NR. He holds a PhD in information security from Aalborg University with focus on secure multi-party cryptographic protocols. He holds a master degree in ICT and an engineering degree in industrial electronics.

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in information and communication technology and applied statistical-mathematical modelling. The clients include a broad range of industrial, commercial and public service organisations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have in us is given by the fact that most of our new contracts are signed with previous customers.

<Name of collaborating institute>

<Info on collaborating institute can go here>

Title	**Security in Android smartphone, Confidentiality in IoT-enabled Smart Grids, and Fault-tolerant privacy-preserving in AMS**
Authors	**Habtamu Abie, Svetlana Boudko, Sigurd Eskeland**
Quality assurance	Wolfgang leister
Date	3. des. 2020
Year	2020
Publication number	DART/07/20

Abstract

This report describes D0.9 “Scientific Paper #6” which consists of three journal papers of which 2 published and 1 submitted. Paper 1 addresses the challenge of security management in Android smartphone platforms, Paper 2 addresses the confidentiality attacks and defences in an Advanced Metering Infrastructure (AMI), and **Paper 3** addresses the problem that “basic” privacy-preserving aggregation schemes lack fault tolerance and that transmission failures or malfunctioning smart meters will prevent aggregation to be successfully conducted for the functioning smart meters of that group, resulting in a complete information loss.

Keywords	Evolutionary game theory, Adaptive security, Confidentiality, IoT-enabled Smart Grids, Fault-tolerant, privacy-preserving
Target group	Research Council of Norway and Partners
Availability	Public
Project number	320548 (248113/O70)

Research field	Anticipatory Adaptive Security for IoT-based Smart Grids
Number of pages	9

Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D 0.9

Security in Android smartphone, Confidentiality in IoT-enabled Smart Grids, and Fault-tolerant privacy-preserving in AMS

Due delivery date: M12

Actual delivery date: M60

Organization name of lead participant for this deliverable:

Norwegian Computing Center

Dissemination level		
PU	Public	**X**
RE	Restricted to a group specified by the consortium	
CO	Confidential, only for members of the consortium	

Deliverable number:	D 0.9
Deliverable responsible:	Habtamu Abie
Work package:	WP0
Editor(s):	Habtamu Abie, Svetlana Boudko, Sigurd Eskeland

Author(s)	
Name	**Organisation**
Svetlana Boudko, Peder Aursand, Habtamu Abie, Sigurd Eskeland	Norwegian Computing Center, Norway
Reijo M. Savola, Markku Kylänpää	VTT Technical Research Centre of Finland

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V01	13.06.2016	Initial input	Habtamu Abie
V1.0	03.12.2020	Final	Habtamu Abie, Svetlana Boudko, Sigurd Eskeland

1 Security in Android smartphone, Confidentiality in IoT-enabled Smart Grids, and Fault-tolerant privacy-preserving in AMS

This deliverable describes D0.9 “Scientific Paper #6” which consists of three journal papers of which 1 published, 1 accepted and 1 submitted. The report summarizes the three journal papers which address security in android smartphone, confidentiality in IoT-enabled smart grids, and fault-tolerant privacy-preserving in AMS, respectively.

Paper 1 [1] addresses the challenge of security management in Android smartphone platforms. Android smartphone is used in various application areas such as public safety, mobile networks, smart homes, smart grids, etc. Therefore, overcoming this challenge is important. This article systematically develops risk-driven security objectives and controls for Android smartphone applications and determines how to offer enough evidence of its security performance via metrics. It also includes conceptualisation and description of adaptive security for an Android platform which can improve the flexibility and effectiveness of these security controls and end-user’s confidence in service providers.

The paper also argues that the successful deployment of mobile applications depends on ensuring security and privacy that need to adapt to the mobile devices’ processing capabilities and resource use. This can be achieved through the development of adaptive and context-aware security for the next generation of digital ecosystems. It used the biological and ecosystem metaphors that provide interesting parallels to the conceptualisations and descriptions of the adaptions, self-adaption and responses which can be at a macroscopic ecosystem level (e.g., system or species) or a microscopic biological level (e.g., molecular, cellular), or at hybrid levels. The self-adaptive component achieves its goal through the following properties:

- **Autonomy**, which allows it to operate without the direct intervention of humans or others and to have some kind of control over its actions and internal state.
- **Social ability**, which allows it to interact with other agents (possibly humans).
- **Reactivity**, which allows it to perceive its environment and respond in a timely fashion to changes that occur in it (the environment)
- **Pro-activeness, learning, and adaptiveness**, which allow it to exhibit goal directed behaviour by taking the initiative, to learn when reacting and/or interacting with its external environment, and to modify its behaviour based on its experience.

The paper contributes to the security of smart home applications that may use Android phones such as eHealth related devices, energy management system, automated transportation, smart closed-circuit television (CCTV), home networks, mobile apps, security applications, and environmental monitoring.

Submission history:

- Submitted to IJICS: 13.06.2016
- Accepted with minor revisions: 23.02.2018
- Submitted revised version: 21.03.2018
- Refereed and accepted for publication in IJICS: 02.08.2018

- Transferred to IJEB: 19.05.2020
- Published: 21.10.2020

Paper 2 [2] addresses the confidentiality attacks and defences in an Advanced Metering Infrastructure (AMI). It has been submitted to the Special Issue "Security and Privacy in IoT Systems (SPIoTS)" that it is now undergoing the first round of the reviewing process. This work is also available as preprint [4]. In this work, we applied evolutionary game theory to extend a resource constrained security game model for confidentiality attacks and defences in an Advanced Metering Infrastructure (AMI), which is a component of IoT-enabled Smart Grids. The AMI is modelled as a tree structure where each node aggregates the information of its children before encrypting it and passing it on to its parent. As a part of the model, we developed a discretization scheme for solving the replicator equations. The aim of this work is to explore the space of possible behaviours of attackers and to develop a framework where the AMI nodes adaptively select the most profitable strategies. Using this model, we simulated the evolution of a population of attackers and defenders on various cases resembling the real-life implementation of AMI. We discuss in depth how to enhance security in AMI using evolutionary game theory either by a priori analysis or as a tool to run dynamic and adaptive infrastructure defence.

Submission history:

- Submitted: 30.10.2020
- Accepted with minor revision: 20.11.2020
- Revised: 01.12.2020

Paper 3 [3] addresses the problem that “basic” privacy-preserving aggregation schemes lack fault tolerance and that transmission failures or malfunctioning smart meters will prevent aggregation to be successfully conducted for the functioning smart meters of that group, resulting in a complete information loss. Aggregation of timeseries consumption data is a widely proposed privacy-preserving measure in the AMI setting. This is relevant as the AMI setting imposes privacy challenges in which smart meters can reveal sensitive information about a person’s presence and activities. This scenario is based on the questionable assumption that the electric utility is fully trusted, which has raised questions and concerns. In this paper, we present a fault-tolerant aggregation scheme, which in cases of failures provides precise aggregate approximations from inputs of remaining functioning meters. Compared to previously proposed fault-tolerant aggregation schemes, this scheme has unsurpassed computational and communication efficiency, as there is only one single encryption per user and no peer-to-peer interaction.

Submission history:

- Submitted: 29.10.2020.
- Resubmitted 27.11.2020 due to problems with the submission system at the first submission.

References

1. Reijo M. Savola, Markku Kylänpää, Habtamu Abie, Risk-driven security metrics for an Android smartphone application. In Int. J. Electronic Business, Vol. 15, No. 4, 2020, pp 297-234. https://doi.org/10.1504/IJEB.2020.111059
2. Svetlana Boudko, Peder Aursand, Habtamu Abie, Evolutionary Game for Confidentiality in IoT-enabled Smart Grids.

3. Sigurd Eskeland, “Fault-tolerant non-interactive privacy-preserving AMS aggregation, submitted to Elsevier’s Journal of Information Security and Applications.
4. Boudko, S.; Aursand, P.; Abie, H. Evolutionary Game for Confidentiality in IoT-enabled Smart Grids. Preprints 2020, 2020110002 (doi: 10.20944/preprints202011.0002.v1)